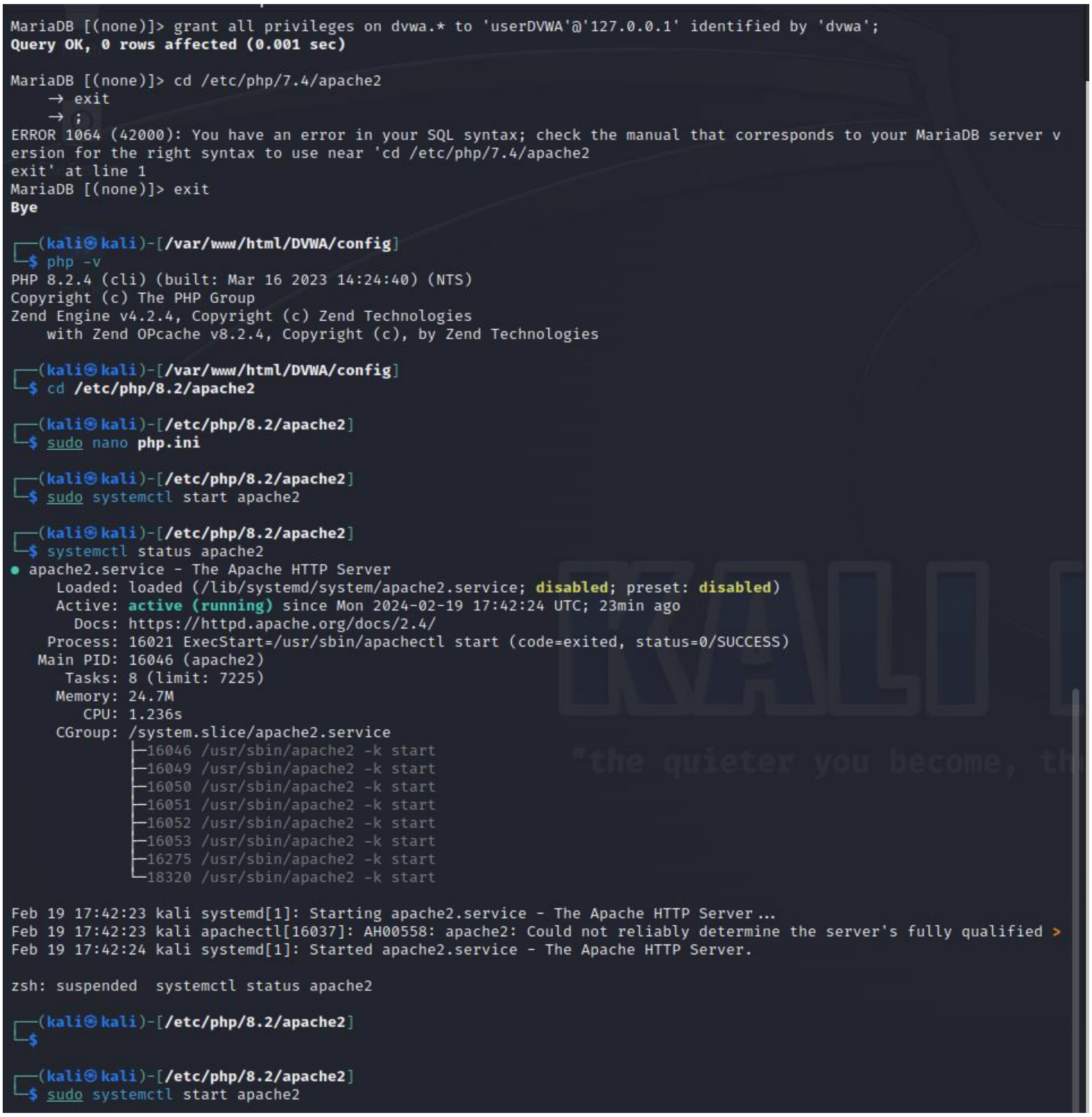
ISM LAB

DVWA

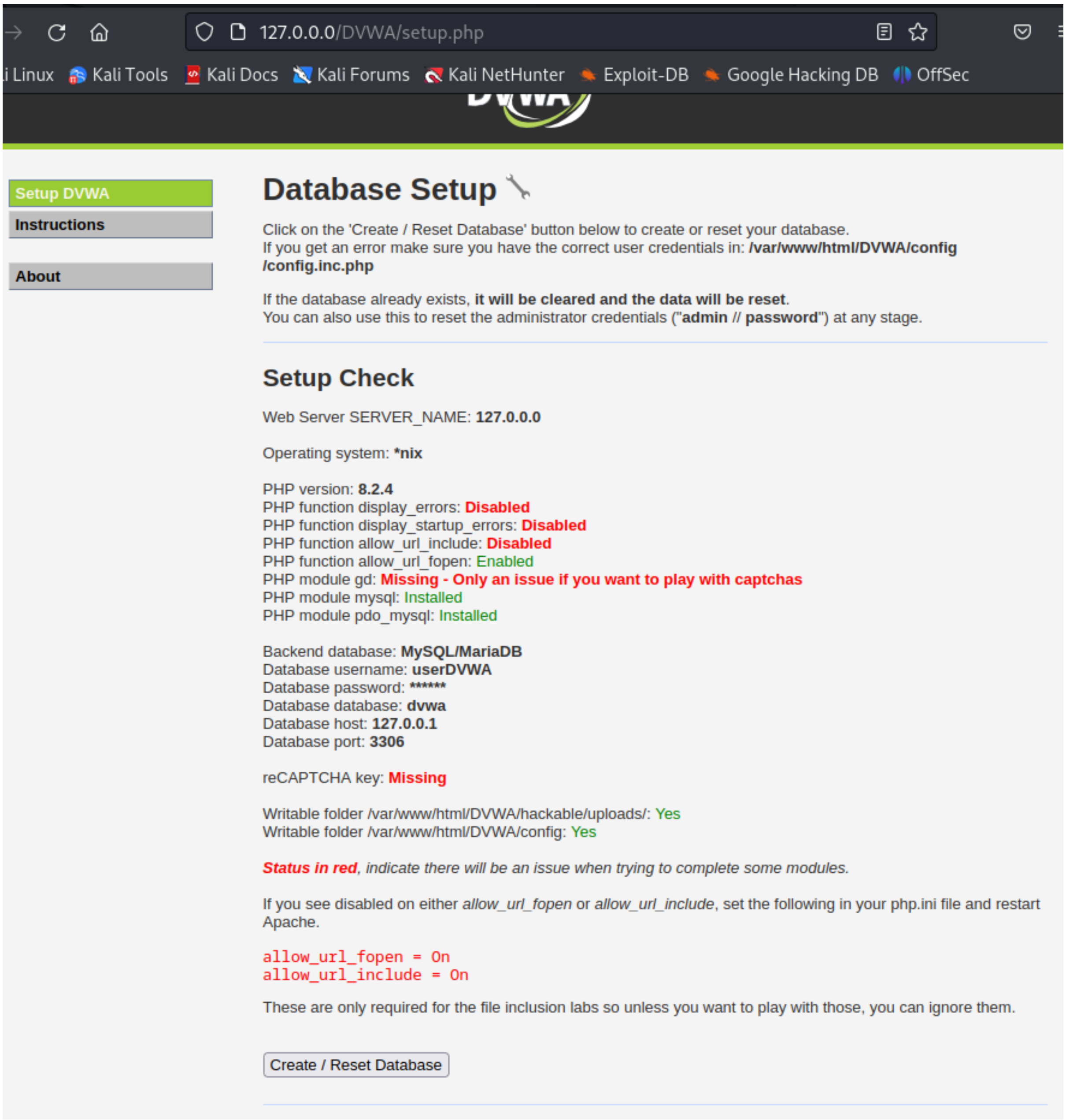
SANTHOSH KRISHNA R

21BCE1651

Installing DVWA



```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> cd /etc/php/7.4/apache2
    → exit
    → ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server v
ersion for the right syntax to use near 'cd /etc/php/7.4/apache2
exit' at line 1
MariaDB [(none)]> exit
Bye

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ php -v
PHP 8.2.4 (cli) (built: Mar 16 2023 14:24:40) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.2.4, Copyright (c) Zend Technologies
    with Zend OPcache v8.2.4, Copyright (c), by Zend Technologies

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ cd /etc/php/8.2/apache2

┌──(kali㉿kali)-[/etc/php/8.2/apache2]
└─$ sudo nano php.ini

┌──(kali㉿kali)-[/etc/php/8.2/apache2]
└─$ sudo systemctl start apache2

┌──(kali㉿kali)-[/etc/php/8.2/apache2]
└─$ systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Mon 2024-02-19 17:42:24 UTC; 23min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 16021 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 16046 (apache2)
      Tasks: 8 (limit: 7225)
     Memory: 24.7M
        CPU: 1.236s
     CGroup: /system.slice/apache2.service
             ├─16046 /usr/sbin/apache2 -k start
             ├─16049 /usr/sbin/apache2 -k start
             ├─16050 /usr/sbin/apache2 -k start
             ├─16051 /usr/sbin/apache2 -k start
             ├─16052 /usr/sbin/apache2 -k start
             ├─16053 /usr/sbin/apache2 -k start
             ├─16275 /usr/sbin/apache2 -k start
             └─18320 /usr/sbin/apache2 -k start

Feb 19 17:42:23 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Feb 19 17:42:23 kali apachectl[16037]: AH00558: apache2: Could not reliably determine the server's fully qualified >
Feb 19 17:42:24 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

zsh: suspended  systemctl status apache2

┌──(kali㉿kali)-[/etc/php/8.2/apache2]
└─$

┌──(kali㉿kali)-[/etc/php/8.2/apache2]
└─$ sudo systemctl start apache2
```



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/DVWA/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Web Server SERVER_NAME: **127.0.0.0**

Operating system: ***nix**

PHP version: **8.2.4**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: **MySQL/MariaDB**
Database username: **userDVWA**
Database password: **********
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**

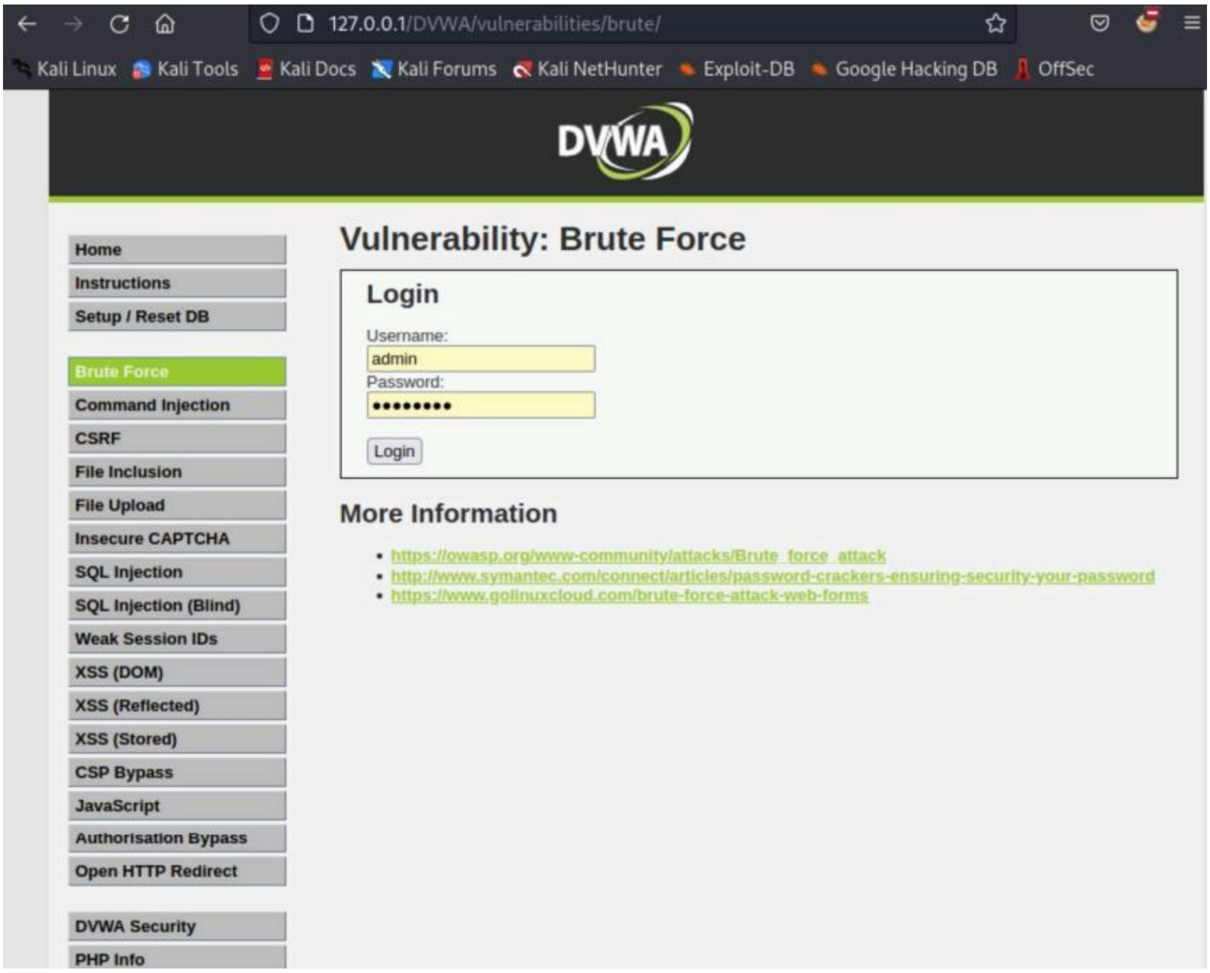
Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
Writable folder /var/www/html/DVWA/config: Yes

Status in red*, indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.



Vulnerability: Brute Force

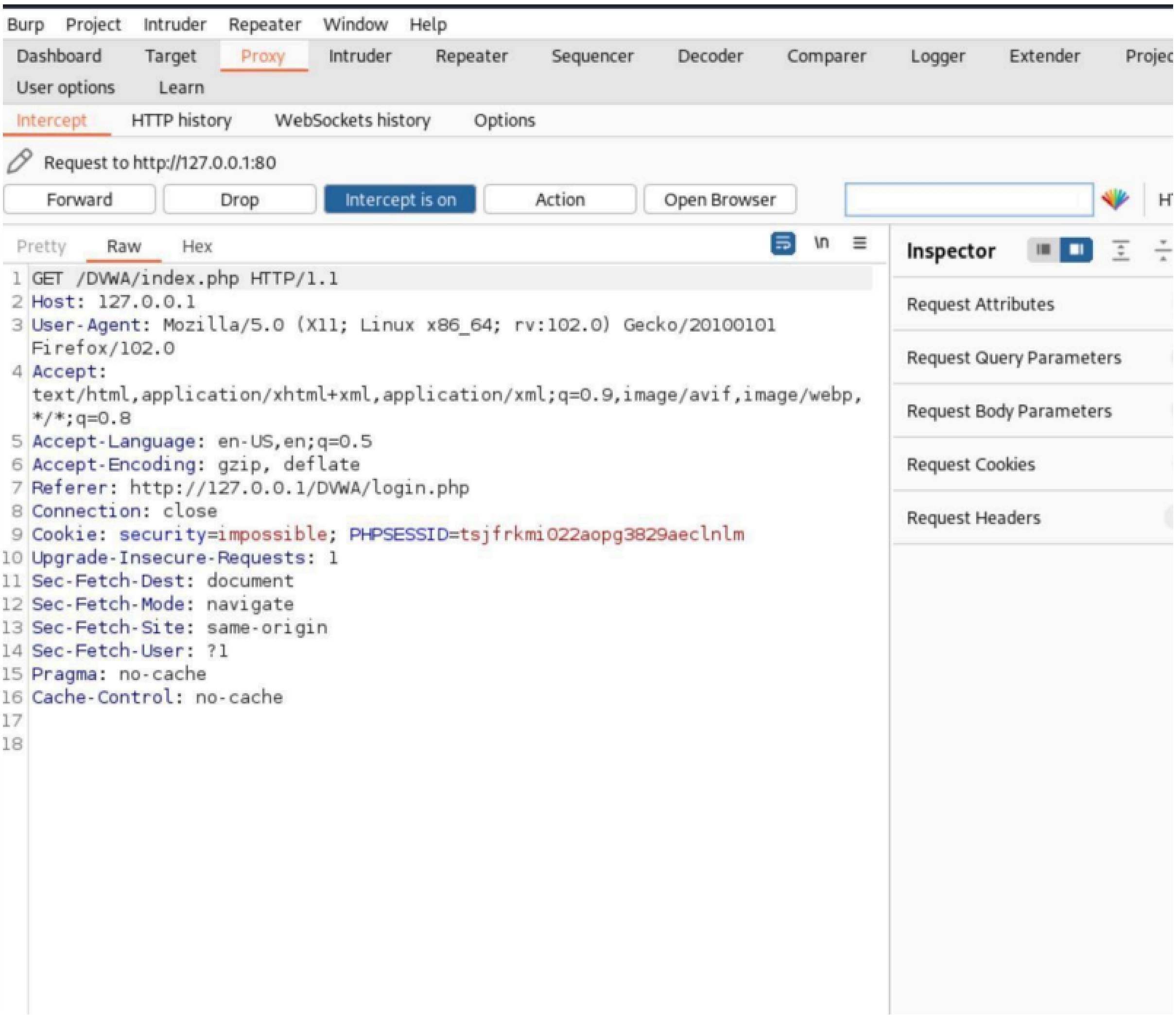
Login

Username: admin

Password: ••••••••••

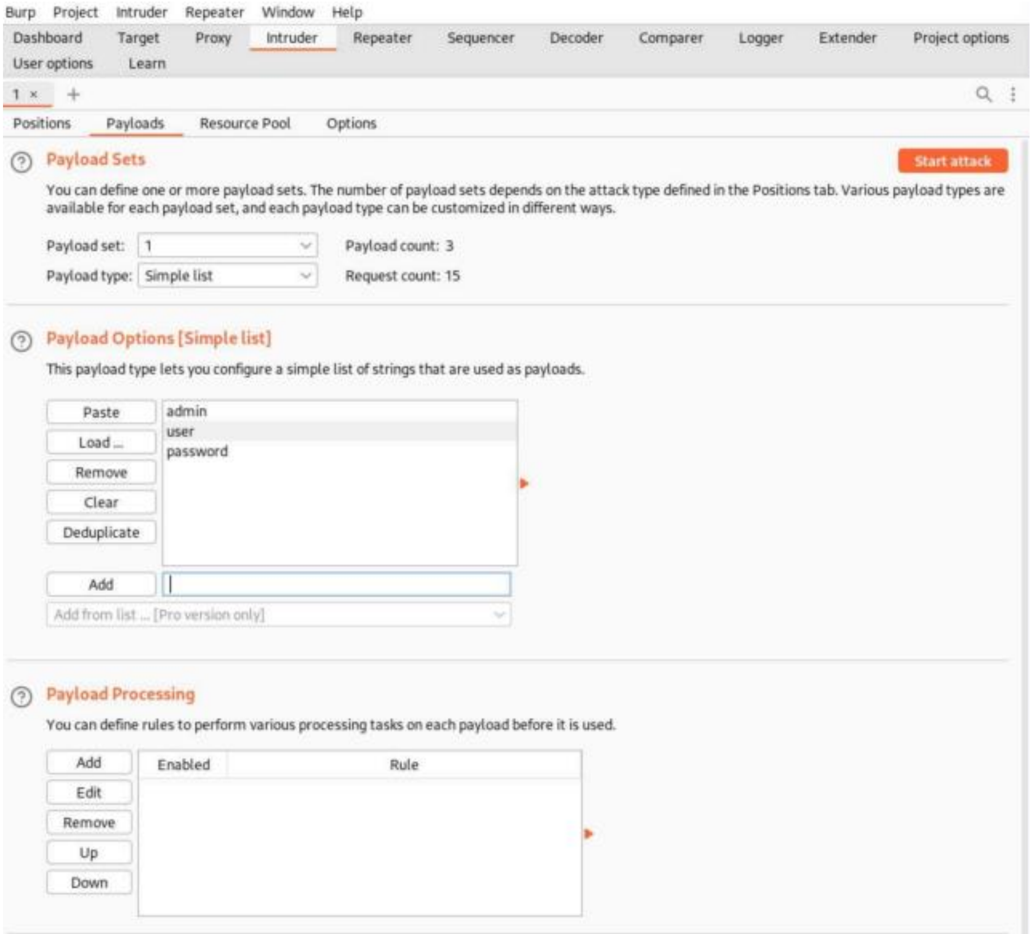
More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- https://www.golinuxcloud.com/brute-force-attack-web-forms


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Projec
User options Learn
Intercept HTTP history WebSockets history Options
Request to http://127.0.0.1:80
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex
\n
Inspector
Request Attributes
Request Query Parameters
Request Body Parameters
Request Cookies
Request Headers

```
GET /DVWA/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/DVWA/login.php
Connection: close
Cookie: security=impossible; PHPSESSID=tsjfrkmi022aopg3829aeclnlm
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Pragma: no-cache
Cache-Control: no-cache


```

1) Sniper attack


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
User options Learn
1 ×
Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ... [Pro version only]
Add
Edit
Remove
Up
Down
Enabled
Rule

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload type: Simple list

Payload count: 3

Request count: 15

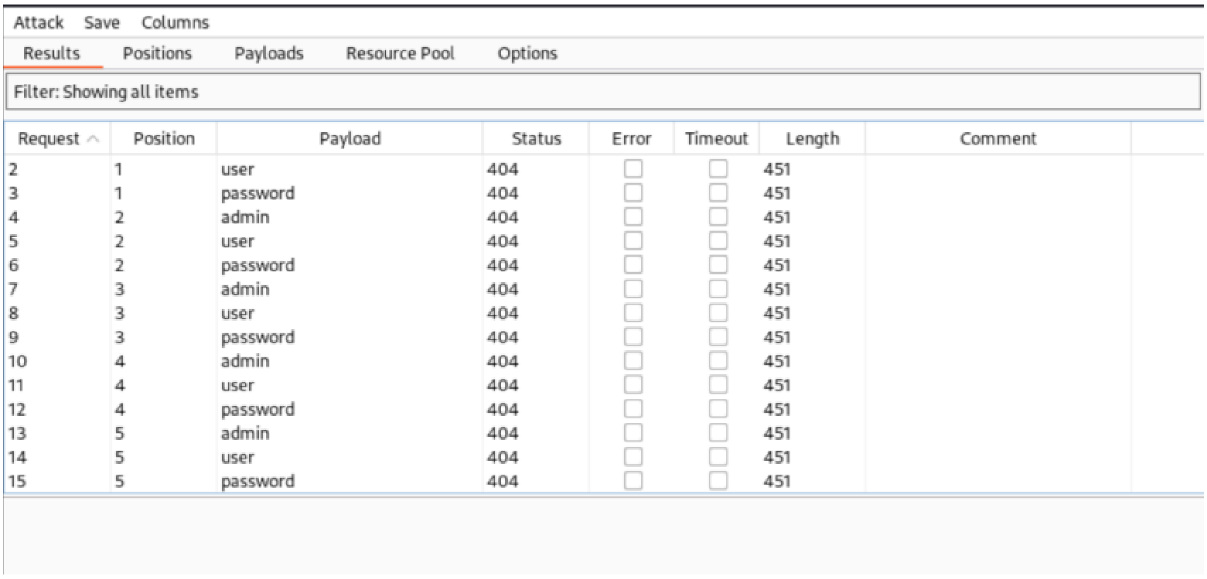
Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

admin
user
password

Payload Processing

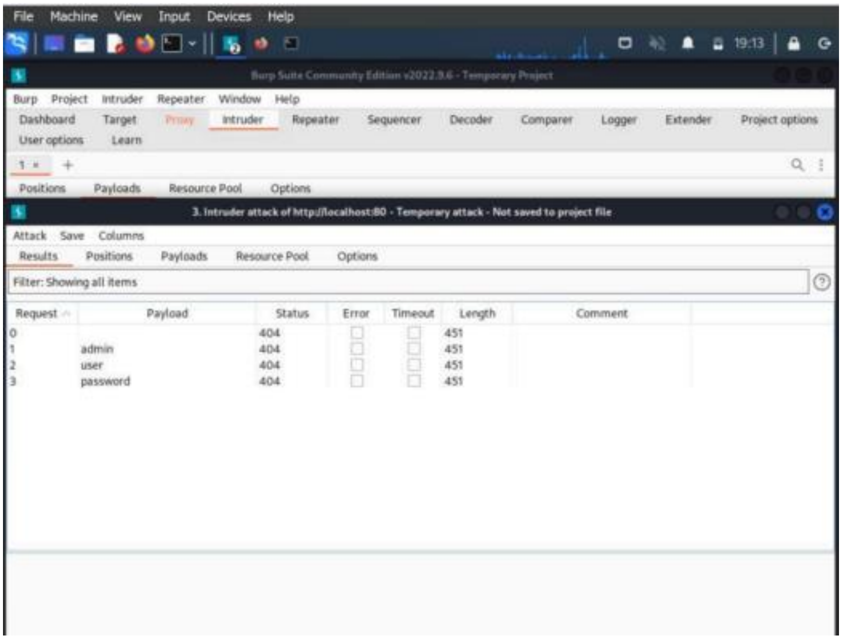
You can define rules to perform various processing tasks on each payload before it is used.



Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
2	1	user	404	☐	☐	451	
3	1	password	404	☐	☐	451	
4	2	admin	404	☐	☐	451	
5	2	user	404	☐	☐	451	
6	2	password	404	☐	☐	451	
7	3	admin	404	☐	☐	451	
8	3	user	404	☐	☐	451	
9	3	password	404	☐	☐	451	
10	4	admin	404	☐	☐	451	
11	4	user	404	☐	☐	451	
12	4	password	404	☐	☐	451	
13	5	admin	404	☐	☐	451	
14	5	user	404	☐	☐	451	
15	5	password	404	☐	☐	451	

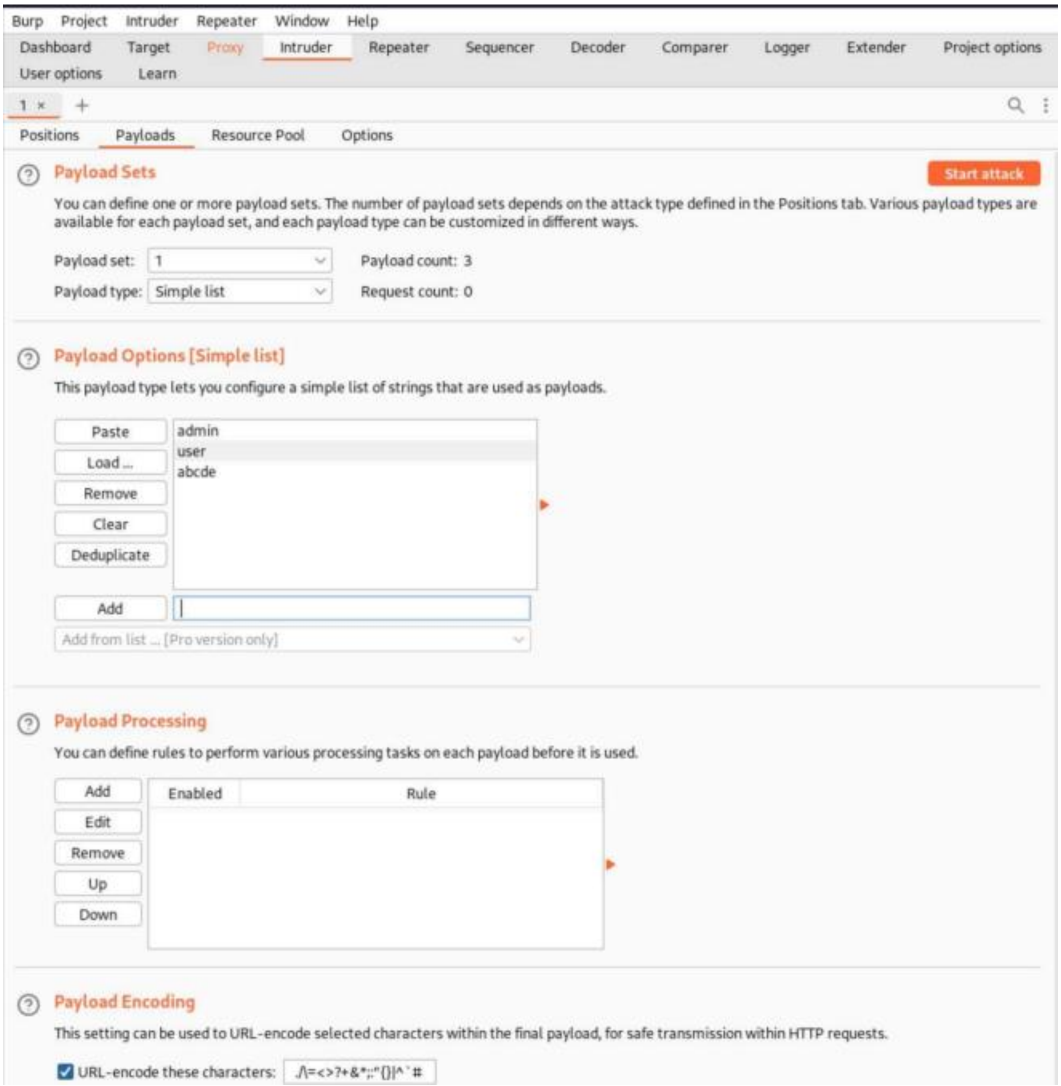
2) Battering Ram


File Machine View Input Devices Help
19:13
Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
User options Learn
1 ×
Positions Payloads Resource Pool Options
3. Intruder attack of http://localhost:80 - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		404	□	□	451	
1	admin	404	□	□	451	
2	user	404	□	□	451	
3	password	404	□	□	451	

3) Pitchfork


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
User options Learn
1 ×
+
Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ... [Pro version only]
Add
Edit
Remove
Up
Down
Enabled
Rule

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 3

Payload type: Simple list

Request count: 0

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
admin
user
abcde
```

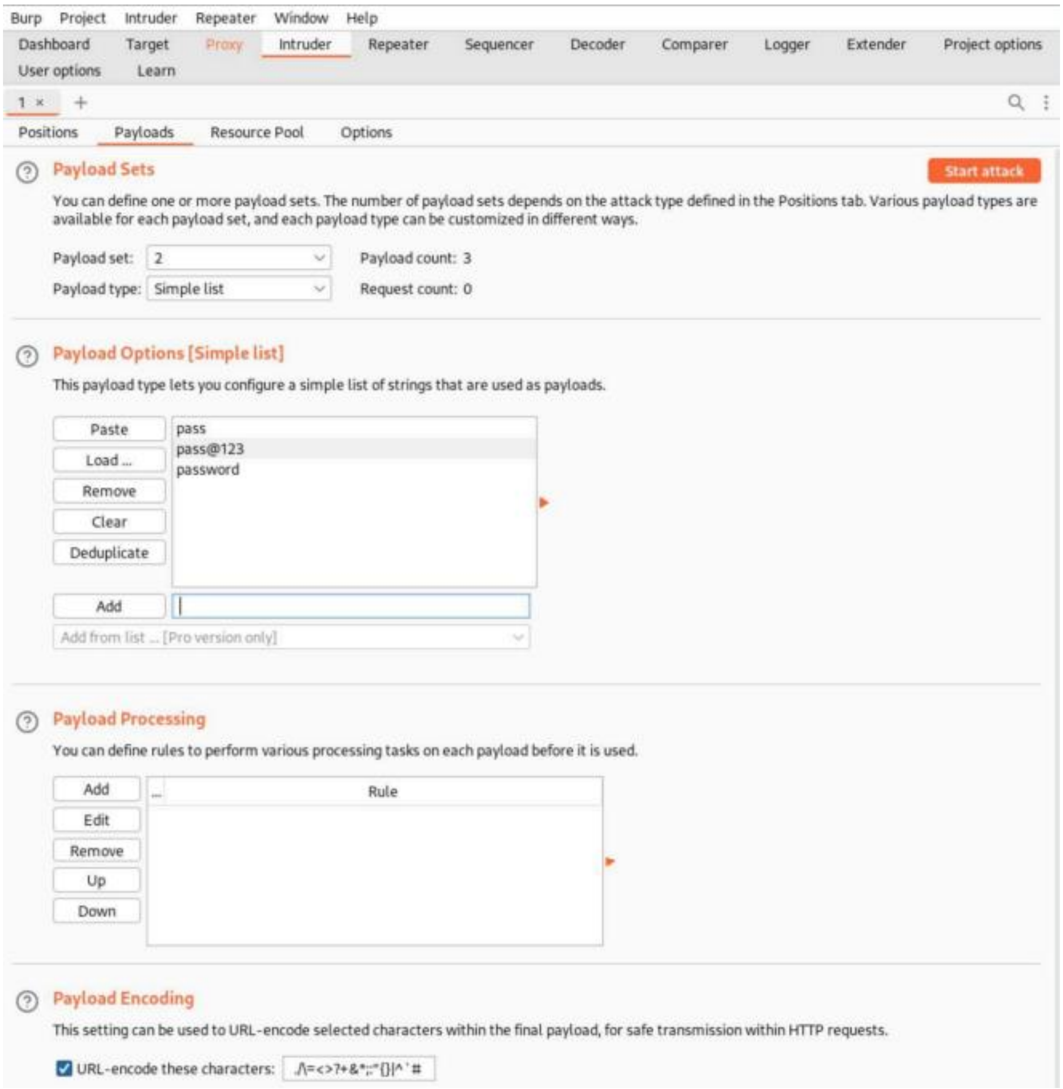
Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
User options Learn
1 × +
Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ... [Pro version only]
Add
Edit
Remove
Up
Down
Rule

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 | Payload count: 3

Payload type: Simple list | Request count: 0

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
pass
pass@123
password
```

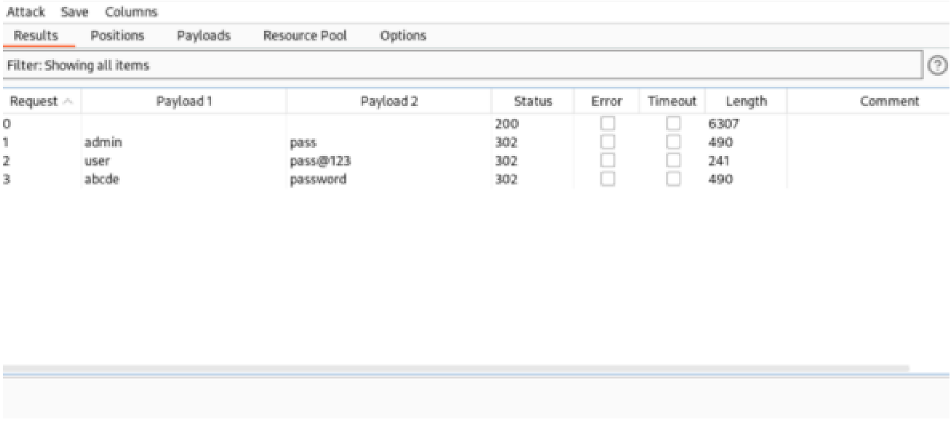
Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

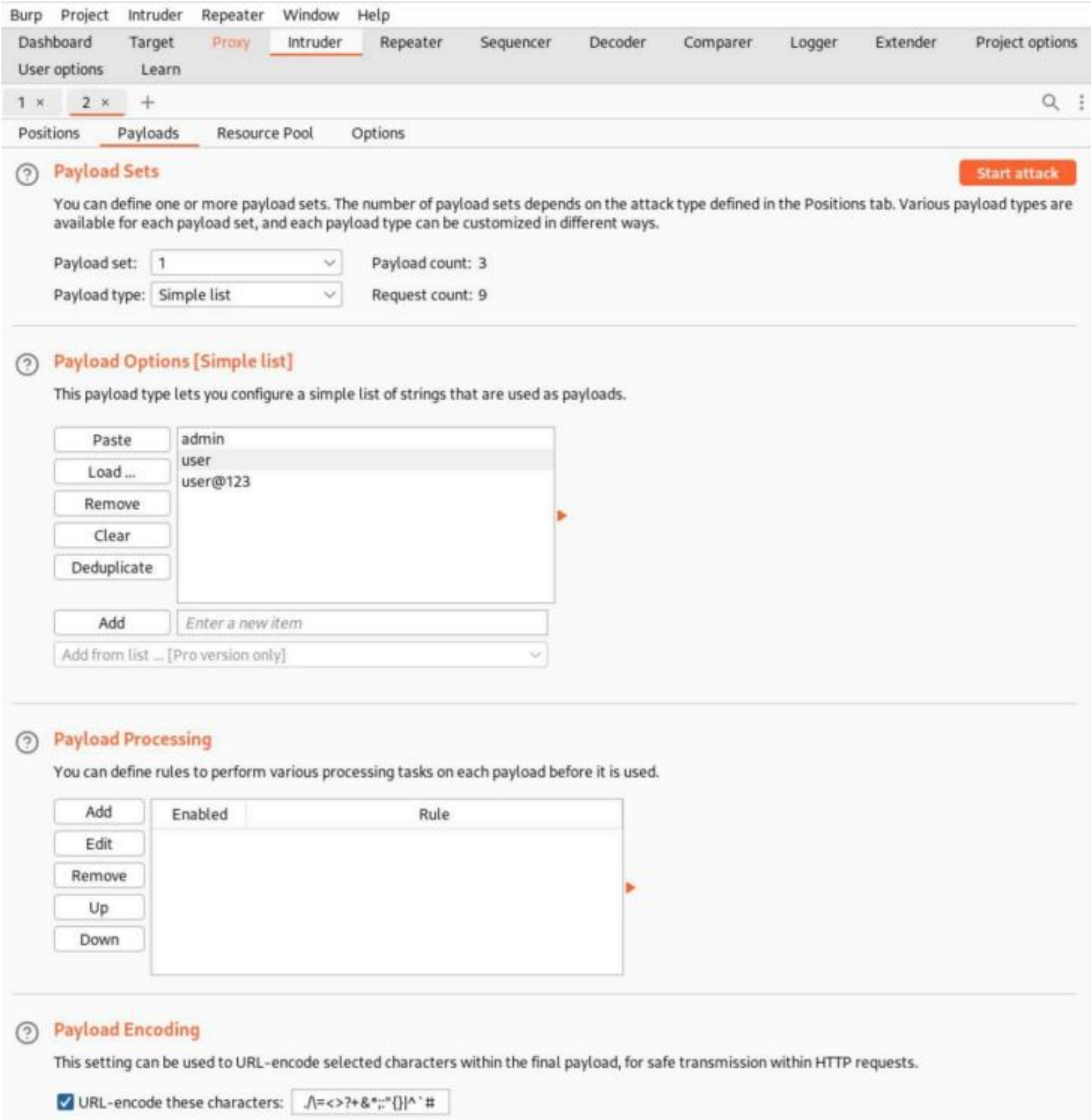
☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#



Filter: Showing all items

Request ^	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	□	□	6307	
1	admin	pass	302	□	□	490	
2	user	pass@123	302	□	□	241	
3	abcde	password	302	□	□	490	

4) Clustering bomb


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
User options Learn
1 × 2 × +
Positions Payloads Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 3

Payload type: Simple list Request count: 9

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
admin
user
user@123
```

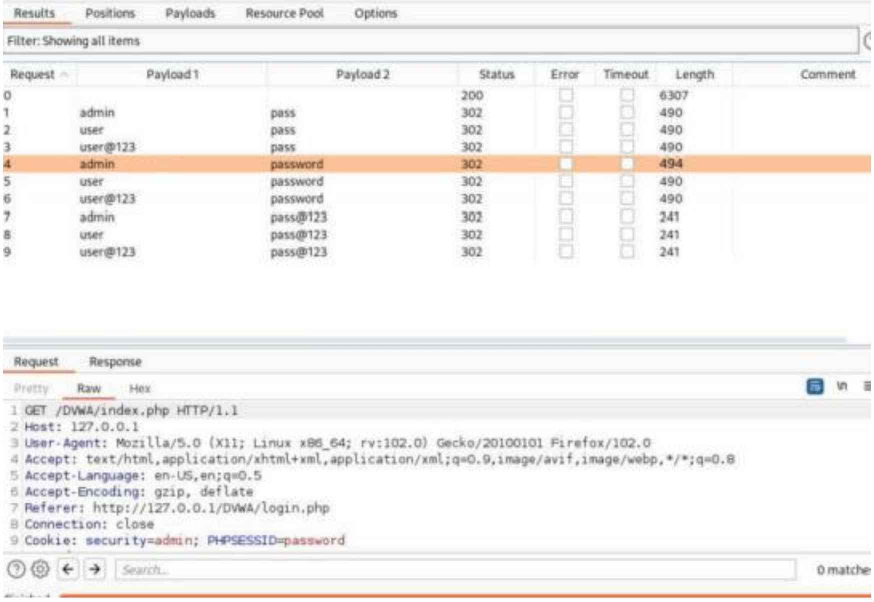
Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#


Results Positions Payloads Resource Pool Options
Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	□	□	6307	
1	admin	pass	302	□	□	490	
2	user	pass	302	□	□	490	
3	user@123	pass	302	□	□	490	
4	admin	password	302	□	□	494	
5	user	password	302	□	□	490	
6	user@123	password	302	□	□	490	
7	admin	pass@123	302	□	□	241	
8	user	pass@123	302	□	□	241	
9	user@123	pass@123	302	□	□	241	

Request Response
Pretty Raw Hex

```
GET /DVWA/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/DVWA/login.php
Connection: close
Cookie: security=admin; PHPSESSID=password
```